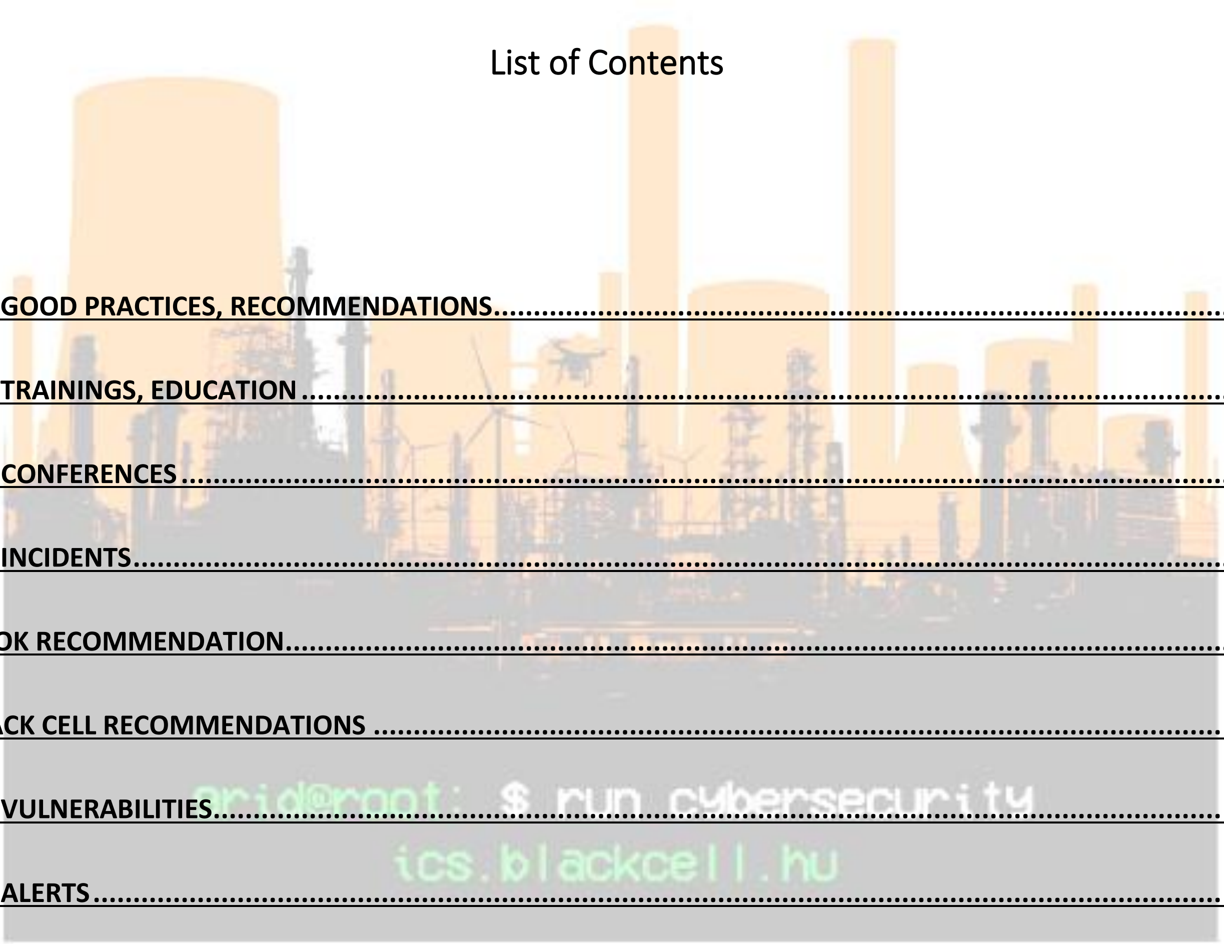
2022. March, Industrial Control Systems security feed

Black Cell is committed for the security of Industrial Control Systems (ICS) and Critical Infrastructure, therefore we are publishing a monthly security feed. This document gives useful information and good practices to the ICS and critical infrastructure operators and provides information on vulnerabilities, trainings, conferences, books, and incidents on the subject of ICS security. Black Cell provides recommendations and solutions to establish a resilient and robust ICS security system in the organization. If you're interested in ICS security, feel free to contact our experts at info@blackcell.io.

List of Contents



ICS GOOD PRACTICES, RECOMMENDATIONS....2

ICS TRAININGS, EDUCATION....3

ICS CONFERENCES....7

ICS INCIDENTS....8

BOOK RECOMMENDATION....9

BLACK CELL RECOMMENDATIONS....10

ICS VULNERABILITIES....11

ICS ALERTS....16

ICS good practices, recommendations

Top 6 ICS Security Best Practices

There are many ICS security best practices. All the best practices give the operators some advice to establish a resilient and secure OT environment. Many are mentioning the same recommendations, but usually one or two new things might be readable in the descriptions.

Garland Technology published one with 6 statements and the following introduction:

Industrial control systems (ICS) are the heart of our world's critical infrastructure, powering everything we enjoy in our connected society. As organizations continue to update their operational technology (OT) with the latest advancements, they should also be aware of the threats that these cyber-physical systems are exposed to. And it's not just the risk of an external attack that should have organizations concerned. They also need to be vigilant about the growing insider threat.

When you consider what could happen if something as important as the supply of electricity, drinking water, food or medicine was disrupted, even just regionally, you can see why it's never been more important to implement strict cybersecurity practices. Here are 6 ICS security best practices you should consider:

1. Establish a Deep Understanding of Each Device in Your Industrial Control Systems
2. Comprehensive Visibility
3. Centralize the Management of User Accounts
4. Automate Vulnerability Management for ICS
5. Implement Anomaly Detection Techniques
6. Empower Security Responders with The Right Data

Source and more information are available on the following link:

https://www.securityweek.com/5-ways-reduce-risk-ransomware-your-ot-network

ICS trainings, education

Without aiming to provide an exhaustive list, the following trainings are available in April 2022:

SANS provides online ICS security courses. The details of the trainings and courses are available on the following link:

https://www.sans.org/course/ics-scada-cyber-security-essentials#results

Periodic online courses:

The Coursera (https://www.coursera.org/) website provides an opportunity to take advantage of online trainings regarding ICS security. The trainings provide video instructions, and the candidates could demonstrate their knowledge in the field of ICS and IoT and the related cloud security. After the course, the University of Colorado, Boulder issues a certificate to the graduates. The following courses are available:

- Developing Industrial Internet of Things Specialization
- Development of Secure Embedded Systems Specialization
- Industrial IoT Markets and Security

More details can be found on the following website:

https://www.coursera.org/search?query=-%09Developing%20Industrial%20Internet%20of%20Things%20Specialization&

ICS CERT offers the following courses:

- Introduction to Control Systems Cybersecurity
- Intermediate Cybersecurity for Industrial Control Systems (201), (202)
- ICS Cybersecurity
- ICS Evaluation

More details can be found on the following website:

https://www.us-cert.gov/ics/Training-Available-Through-ICS-CERT

ICS-CERT Virtual Learning Portal (VLP) provides the following short courses:

- Operational Security (OPSEC) for Control Systems (100W) - 1 hour
- Differences in Deployments of ICS (210W-1) – 1.5 hours
- Influence of Common IT Components on ICS (210W-2) – 1.5 hours
- Common ICS Components (210W-3) – 1.5 hours
- Cybersecurity within IT & ICS Domains (210W-4) – 1.5 hours
- Cybersecurity Risk (210W-5) – 1.5 hours
- Current Trends (Threat) (210W-6) – 1.5 hours
- Current Trends (Vulnerabilities) (210W-7) – 1.5 hours

- Determining the Impacts of a Cybersecurity Incident (210W-8) – 1.5 hours
- Attack Methodologies in IT & ICS (210W-9) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 1 (210W-10) – 1.5 hours
- Mapping IT Defense-in-Depth Security Solutions to ICS - Part 2 (210W-11) – 1.5 hours
- Industrial Control Systems Cybersecurity Landscape for Managers (FRE2115) - 1 hour

VLP courses are available on the same website, like the other ICS-CERT courses.

SANS online courses in the field of ICS security:

- ICS410: ICS/SCADA Security Essentials
  - 10-15. April 2022
  - anytime, on demand.

- ICS515: ICS Active Defense and Incident Response
  - anytime, on demand.

More details can be found on the following website:

https://www.sans.org/find-training/search?types=10&coursecode=ICS410,ICS515

Udemy provides online courses in ICS and SCADA security. From the basics of ICS and SCADA security principles to the technological solutions and governance questions, the below course could help to understand the essence of the ICS/SCADA security.

- ICS/SCADA Cyber Security
- Learn SCADA from Scratch to Hero (Indusoft & TIA portal)
- Fundamentals of OT Cybersecurity (ICS/SCADA)

More details can be found on the following website:

https://www.udemy.com/ics-scada-cyber-security/

The **Department of Homeland Security's** two days training is useful for the ICS/SCADA operators:

- SCADA security training

The courses are available live online.

More details can be found on the following website:

https://www.tonex.com/training-courses/scada-security-training/

The **SCADAhacker.com** website provides ICS security online courses:

- Fundamentals of Industrial Control System Cyber Security

The training takes 40-120 hours, and 8 modules can help to understand the ICS cybersecurity issues. The training focuses on the „Blue teaming" activities, for ICS and SCADA systems.

If you have a certificate, like CISSP or CEH, the course can help to add some ICS and SCADA specific knowledge.

More details can be found on the following website:

https://scadahacker.com/training.html

INFOSEC-Flex SCADA/ICS Security Training Boot Camp gives the possibility for ICS/SCADA operators to get ready for external and internal threats.

The 4 days course guarantees the "Certified SCADA Security Architect" certification for the candidates (93% exam pass rate).

The basics of the ICS/SCADA security, governance, security controls, penetration testing and other topics can help the participants to become an ICS/SCADA security expert.

More details can be found on the following website:

https://www.infosecinstitute.com/courses/scada-security-boot-camp/

Industrial Control System (ICS) & SCADA Cyber Security Training

This is a three day course, what is designed for:

- IT and ICS cybersecurity personnel
- Field support personnel and security operators
- Auditors, vendors and team leaders
- Electric utility engineers
- System personnel & System operators
- Independent system operator personnel
- Electric utility personnel involved with ICS security.
- Technicians, operators, and maintenance personnel
- Investors and contractors in the electric industry
- Managers, accountants, and executives of electric industry

More details can be found on the following website:

https://www.tonex.com/training-courses/industrial-control-system-scada-cybersecurity-training/

Bsigroup: Certified Lead SCADA Security Professional training course

This five-day training course will enable you to develop the expertise to plan, design and implement an effective programme to protect SCADA systems. You'll gain an understanding of common Industrial Control Systems (ICS) threats, vulnerabilities, and risks, and how they can be managed.

By attending this course you'll gain the knowledge and skills to advise on or manage risks related to SCADA environments and systems as a qualified professional. On successful completion of the PECB exam that takes place on the final day of this course, you'll gain Certified Lead SCADA Security Professional status.

Duration: 5 days, anytime at your office

More details can be found on the following website:

https://www.bsigroup.com/en-GB/our-services/digital-trust/cybersecurity-information-resilience/Training/certified-lead-scada-security-professional/

ICS/SCADA security training seminar

The courses are derived from 28 years of first-hand technology experience and industry best practices. The classes are customized to your team’s requirements and taught at your offices, classrooms and online live by world-class instructors with publications, patents, awards/honors, and a passion to share knowledge.

More details can be found on the following website:

https://www.enoinstitute.com/scada-ics-security-training-seminar/

ICS conferences

In April 2022, the following ICS/SCADA security conferences and workshops will be organized (not comprehensive):

ICCSICS 2022: 16. International Conference on Cyber Security of Industrial Control Systems

The International Research Conference is a federated organization dedicated to bringing together a significant number of diverse scholarly events for presentation within the conference program. Events will run over a span of time during the conference depending on the number and length of the presentations. With its high quality, it provides an exceptional value for students, academics and industry researchers.

International Conference on Cyber Security of Industrial Control Systems aims to bring together leading academic scientists, researchers and research scholars to exchange and share their experiences and research results on all aspects of Cyber Security of Industrial Control Systems. It also provides a premier interdisciplinary platform for researchers, practitioners and educators to present and discuss the most recent innovations, trends, and concerns as well as practical challenges encountered and solutions adopted in the fields of Cyber Security of Industrial Control Systems.

Venice, Italy; April 14th -15th, 2022

More details can be found on the following website:

https://waset.org/cyber-security-of-industrial-control-systems-conference-in-april-2022-in-venice

Cyber Security for Critical Assets APAC

The coronavirus pandemic has caused a surge in cyberthreats and attacks, a lot of which have targeted companies whose employees must now access critical infrastructure, such as industrial control systems (ICS) and operational technology (OT) networks, from home. But that critical infrastructure, which keeps modern society going even during a pandemic, is seriously under- protected against cyberattacks. Providing the collaboration platform and expertise needed to address these new circumstances, the globally acclaimed Cyber Security for Critical Assets summit returns to Singapore for its 3rd Asian Pacific edition in 2022.

CS4CA APAC unites IT & OT security leaders to network, learn and collaborate towards cyber resilience by exchanging first-hand expert information and joining forces in addressing common concerns. Senior experts share first-hand insights through real-life case studies, panel debates, and keynote presentations, while bringing forth urgent topics to be discussed over roundtables and networking breaks.

Singapore, Singapore; April 26th -27th, 2022

More details can be found on the following website:

https://apac.cs4ca.com/

ICS incidents

Ransomware gang breached 52 US critical infrastructure providers

The US Federal Bureau of Investigation (FBI) says the Ragnar Locker ransomware gang has breached the networks of at least 52 organizations from multiple US critical infrastructure providers. The sectors for the providers are the following: critical manufacturing, energy, financial services, government, and information technology.

The indicators of compromise (IoC) detailed in the flash report, what is available on the following link: https://www.ic3.gov/Media/News/2022/220307.pdf

Ragnar Locker operators terminate remote management software (e.g., ConnectWise, Kaseya) used by managed service providers (MSPs) to manage clients' systems remotely on compromised enterprise endpoints.

This allows the threat actors to evade detection and make sure remotely logged-in admins do not interfere with or block the ransomware deployment process.

This new strain of Ragnar is quite unique as it’s using an old version of SUN (now Oracle) Virtualbox hypervisor to deploy a Windows XP VM image to control and spread the infection (https://news.sophos.com/en-us/2020/05/21/ragnar-locker-ransomware-deploys-virtual-machine-to-dodge-security/)

To defend against this strain, we suggest to monitor the files mentioned in the above article and block them on computers, which do not need to run VirtualBox.

FBI still recommend that nobody pay for the extortioners.

The source and more information available on the following link:

https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/

Book recommendation

InduSoft Application Design and SCADA Deployment Recommendations for Industrial Control System Security

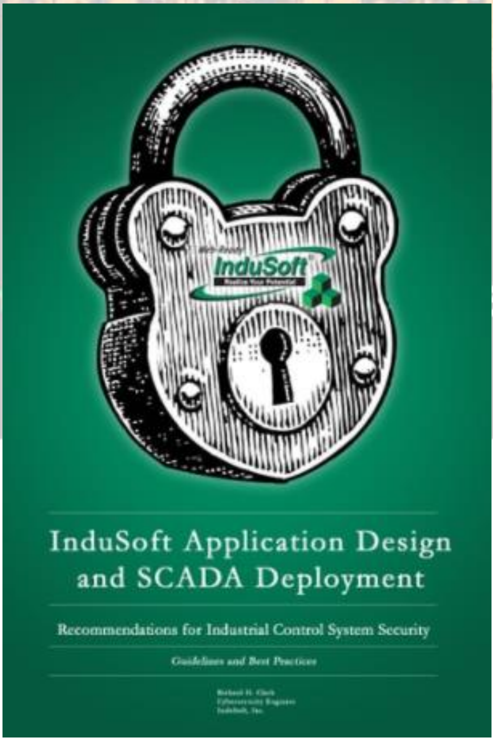
InduSoft conducts ongoing product and informational SCADA security webinars, publish Technical Notes and White Papers on application construction and security related topics, and publishes corporate blogs on security and a number of other useful topics by a variety of different authors. Topics from various InduSoft publications and other media are presented in this eBook to help you with your SCADA design and security issues. There are links within the topics that will take you to more in-depth information that is not presented in this handbook. Feel free to explore any of the topics and subjects in more depth by simply clicking on the links provided within the sections and in the footnotes provided for you.

Authors/Editors: Richard Clark.

Year of issue: 2015

The book is available at the following link:

https://www.kobo.com/us/en/ebook/indusoft-application-design-and-scada-deployment-recommendations-for-industrial-control-system-security


InduSoft
InduSoft Application Design and SCADA Deployment
Recommendations for Industrial Control System Security
Guidelines and Best Practices

Black Cell recommendations

Shadowserver Starts Conducting Daily Scans to Help Secure ICS

Securityweek published an article about a non-profit organization, which can help to identify the industrial control system operators to find the vulnerabilities.

Shadowserver Foundation has started conducting daily internet scans in an effort to identify exposed industrial control systems (ICS) and help organizations reduce their exposure to attacks.

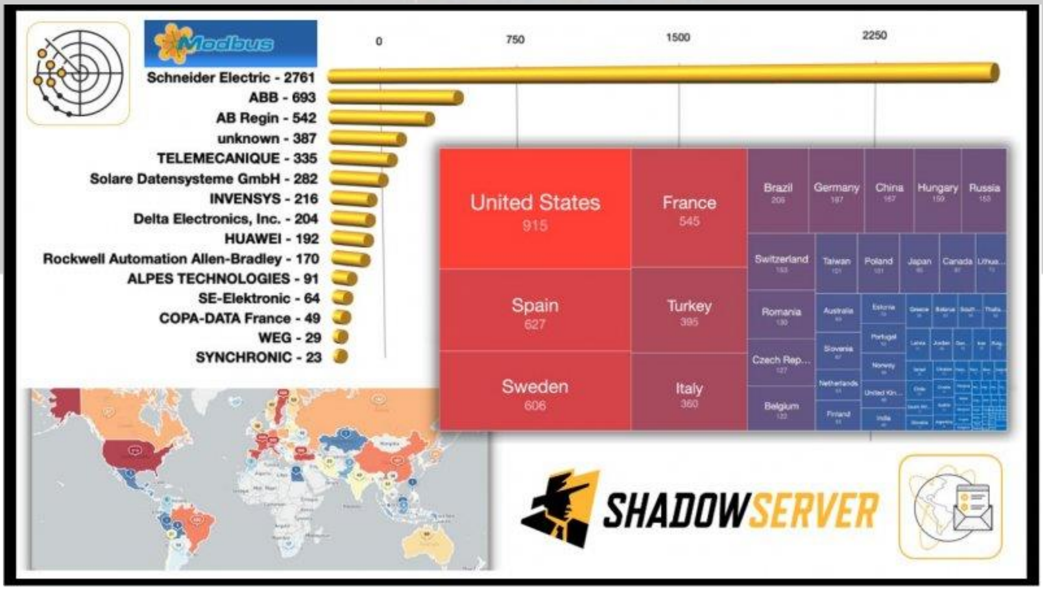
For now, Shadowserver Foundation scanning the web for exposed services that use the Modbus industrial communications protocol on TCP port 502, but the near future this service will be extends other ICS and operational technology protocols.

The first daily ICS scan conducted by Shadowserver revealed more than 6,300 unique IP addresses corresponding to exposed Modbus services. A majority are associated with Siemens products, followed by ABB, AB Regin, Schneider Electric’s Telemecanique, Solare Datensysteme, Invensys, Delta Electronics, Huawei, Rockwell Automation (Allen Bradley), Alpes Technologies, SE-Elektronic, COPA-DATA, WEG, and Synchronic.

We strongly recommend following Shadowserver Foundation on the social media platforms, particularly on twitter.

Source and more details available on the following link:

https://www.securityweek.com/shadowserver-starts-conducting-daily-scans-help-secure-ics



ICS vulnerabilities

In March 2021, the following vulnerabilities were reported by the National Cybersecurity and Communications Integration Center, Industrial Control Systems (ICS) Computer Emergency Response Teams (CERTs) – ICS-CERT:

ICSMA-22-088-01: Philips e-Alert

Medium level vulnerability: Missing Authentication for Critical Function.
https://www.cisa.gov/uscert/ics/advisories/icsma-22-088-01

ICSA-22-088-01: Rockwell Automation ISaGRAF

Medium level vulnerability: Improper Restriction of XML External Entity Reference.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-01

ICSA-22-088-02: Omron CX-Position

High level vulnerabilities: Stack-based Buffer Overflow, Improper Restriction of Operations Within the Bounds of a Memory Buffer, Use After Free, Out-of-bounds Write.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-02

ICSA-22-088-03: Hitachi Energy LinkOne WebView

Low level vulnerabilities: Cross-site Scripting, Use of a Password System for Primary Authentication, Configuration, Exposure of Sensitive Information to an Unauthorized Actor.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-03

ICSA-22-088-04: Modbus Tools Modbus Slave

Medium level vulnerability: Stack-based Buffer Overflow.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-088-04

ICSA-22-081-01: Delta Electronics DIAEnergie (Update A)

Critical level vulnerabilities: Path Traversal, Incorrect Default Permissions, SQL Injection, Uncontrolled Search Path Element.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01

ICSA-22-083-01: Yokogawa CENTUM and Exaopc

High level vulnerabilities: Use of Hard-coded Credentials, Relative Path Traversal, Improper Output Neutralization for Logs, OS Command Injection, Permissions, Privileges, and Access Controls, Uncontrolled Search Path Element.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-083-01

ICSA-22-083-02: mySCADA myPRO

High level vulnerability: Command Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-083-02

ICSA-22-081-01: Delta Electronics DIAEnergie

Critical level vulnerabilities: Path Traversal, Incorrect Default Permissions, SQL Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-081-01

ICSA-21-238-03: Delta Electronics DIAEnergie (Update B)

Critical level vulnerabilities: Use of Password Hash with Insufficient Computational Effort, Authentication Bypass Using an Alternate Path or Channel, Unrestricted Upload of File with Dangerous Type, SQL Injection, Cross-site Request Forgery, Cross-site Scripting, Cleartext Transmission of Sensitive Information.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-238-03

ICSA-20-168-01: Treck TCP/IP Stack (Update H)
Critical level vulnerabilities: Improper Handling of Length Parameter Inconsistency, Improper Input Validation, Double Free, Out-of-bounds Read, Integer Overflow or Wraparound, Improper Null Termination, Improper Access Control.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-168-01

ICSA-22-074-01: ABB OPC Server for AC 800M
High level vulnerability: Execution with Unnecessary Privileges.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-074-01

ICSA-22-067-01: PTC Axeda agent and Axeda Desktop Server (Update B)
Critical level vulnerabilities: Use of Hard-coded Credentials, Missing Authentication for Critical Function, Exposure of Sensitive Information to an Unauthorized Actor, Path Traversal, Improper Check or Handling of Exceptional Conditions.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01

ICSA-22-069-01: Siemens RUGGEDCOM Devices
Medium level vulnerability: Missing Encryption of Sensitive Data.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-01

ICSA-22-069-02: Siemens SIMOTICS CONNECT 400
High level vulnerabilities: Type Confusion, Improper Validation of Specified Quantity in Input, Wrap or Wraparound, Improper Handling of Inconsistent Structural Elements.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-02

ICSA-22-069-03: Siemens SINEC NMS
High level vulnerabilities: SQL Injection, Deserialization of Untrusted Data, Improper Privilege Management.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-03

ICSA-22-069-04: Siemens SINEMA Mendix Forgot Password Appstore
Critical level vulnerabilities: Improper Access Control, Improper Restriction of Excessive Authentication Attempts.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-04

ICSA-22-069-05: Siemens Simcenter STAR-CCM+ Viewer
High level vulnerability: Improper Restriction of Operations within the Bounds of a Memory Buffer.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-05

ICSA-22-069-06: **Siemens COMOS**

High level vulnerabilities: Memory Allocation with Excessive Size Value, Untrusted Pointer Dereference, Type Confusion, Stack-based Buffer Overflow, Out-of-bounds Write, Out-of-bounds Read, Use After Free, Improper Check for Unusual or Exceptional Conditions.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-06

ICSA-22-069-07: **Siemens Climatix POL909**

Medium level vulnerabilities: Cross-site Scripting, Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-07

ICSA-22-069-08: **Siemens Polarion ALM**

Medium level vulnerability: Cross-site Scripting.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-08

ICSA-22-069-09: **Siemens SINEC INS**

Critical level vulnerability: Using Components with Known Vulnerabilities.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-09

ICSA-22-069-10: **Siemens Simcenter Femap**

High level vulnerabilities: Out-of-bounds Write, Stack-based Buffer Overflow.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-10

ICSA-22-069-11: **Siemens SINUMERIK MC**

High level vulnerability: Improper Privilege Management.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-11

ICSA-22-069-12: **Siemens RUGGEDCOM ROS**

High level vulnerability: Using Components with Known Vulnerabilities.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-12

ICSA-22-069-13: **Siemens Mendix**

Medium level vulnerability: Improper Access Control.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-069-13

ICSA-22-041-01: **Siemens SIMATIC Industrial Products** (Update A)

High level vulnerabilities: Operation on a Resource after Expiration or Release, Missing Release of Memory after Effective Lifetime.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-01

ICSA-22-041-05: **Siemens SICAM TOOLBOX II** (Update A)

Critical level vulnerability: Use of Hard-coded Credentials.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-05

ICSA-22-041-07: **Siemens Solid Edge, JT2Go, and Teamcenter Visualization**

High level vulnerabilities: Improper Restriction of Operations within the Bounds of a Memory Buffer, Out-of-bounds Write, Heap-based Buffer Overflow, Out-of-bounds Read.

https://www.cisa.gov/uscert/ics/advisories/icsa-22-041-07

ICSA-21-315-03: **Siemens SIMATIC WinCC** (Update B)

Critical level vulnerabilities: Path Traversal, Insertion of Sensitive Information into Log File.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-03

ICSA-21-315-09: **Siemens Climatix POL909** (Update A)

Medium level vulnerability: Missing Encryption of Sensitive Data.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-315-09

ICSA-21-222-05: **Siemens Industrial Products Intel CPUs** (Update B)

High level vulnerability: Missing Encryption of Sensitive Data.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-222-05

ICSA-21-103-13: **Siemens SIMOTICS CONNECT 400** (Update A)

Medium level vulnerabilities: Improper Null Termination, Out-of-bounds Read, Access of Memory Location After End of Buffer, Use of Insufficiently Random Values.
https://www.cisa.gov/uscert/ics/advisories/icsa-21-103-13

ICSA-20-252-07: **Siemens Industrial Products** (Update F)

Medium level vulnerability: Exposure of Sensitive Information to an Unauthorized Actor.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-252-07

ICSA-20-203-01: **Wibu-Systems CodeMeter** (Update F)

Critical level vulnerabilities: Buffer Access with Incorrect Length Value, Inadequate Encryption Strength, Origin Validation Error, Improper Input Validation, Improper Verification of Cryptographic Signature, Improper Resource Shutdown or Release.
https://www.cisa.gov/uscert/ics/advisories/icsa-20-203-01

ICSA-19-253-03: **Siemens Industrial Products** (Update P)

High level vulnerabilities: Excessive Data Query Operations in a Large Data Table, Integer Overflow or Wraparound, Uncontrolled Resource Consumption.
https://www.cisa.gov/uscert/ics/advisories/icsa-19-253-03

ICSA-22-067-01: **PTC Axeda agent and Axeda Desktop Server**

Critical level vulnerabilities: Use of Hard-coded Credentials, Missing Authentication for Critical Function, Exposure of Sensitive Information to an Unauthorized Actor, Path Traversal, Improper Check or Handling of Exceptional Conditions.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-01

ICSA-22-067-02: **AVEVA System Platform**

High level vulnerability: Cleartext Storage of Sensitive Information in Memory.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-067-02

ICSA-22-034-01: **Sensormatic PowerManage** (Update A)

Critical level vulnerability: Improper Input Validation.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-034-01

ICSA-22-063-01: Trailer Power Line Communications (PLC) J2497

Critical level vulnerabilities: Missing Authentication for Critical Function, Improper Protection against Electromagnetic Fault Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-063-01

ICSMA-22-062-01: BD Pyxis

High level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsma-22-062-01

ICSMA-22-062-02: BD Viper LT

High level vulnerability: Use of Hard-coded Credentials.
https://www.cisa.gov/uscert/ics/advisories/icsma-22-062-02

ICSA-22-062-01: IPCOMM ipDIO

High level vulnerabilities: Cross-site Scripting, Code Injection.
https://www.cisa.gov/uscert/ics/advisories/icsa-22-062-01

The vulnerability reports contain more detailed information, which can be found on the following website:

https://ics-cert.us-cert.gov/advisories

Continuous monitoring of vulnerabilities is recommended, because relevant information on how to address vulnerabilities, patch vulnerabilities and mitigate risks are also included in the detailed descriptions.

ICS alerts

In March 2022, ICS-CERT has not published alerts.

The previous alerts can be found at the following link:

https://www.us-cert.gov/ics/alerts